IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALVARO AMIGON, Plaintiff, vs. **OLD DOMINION FREIGHT LINE, INC.**, Defendant.	Case No.: 1:24-cv-01934 **JURY TRIAL DEMANDED**

COMPLAINT

ALVARO AMIGON ("Plaintiff"), through counsel, for his Complaint against Defendant, OLD DOMINION FREIGHT LINE, INC. ("Defendant"), their subsidiaries and affiliates, states:

NATURE OF THE CASE

1. This is an action to recover statutory damages and for injunctive relief arising out of unlawful collection, receipt, use, possession, retention and disclosure of the personal biometric identifiers and biometric information of Plaintiff in violation of the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1 (2008).

THE PARTIES

2. Plaintiff is a natural person and is domiciled in Illinois.

3. Defendant, OLD DOMINION FREIGHT LINE, INC., is a foreign corporation, organized under the laws of the State of Virginia, with its principal place of business located in Thomasville, North Carolina. Defendant is registered with the Illinois Secretary of State and conducts business in the State of Illinois.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a) as the matter in controversy exceeds $75,000.00[1] exclusive of punitive damages, and/or interest and costs, and is between citizens of different States.

5. Plaintiff is a citizen of Illinois. Defendant is a Virginia corporation with its corporate headquarters located in Thomasville, North Carolina.

6. This Court has personal jurisdiction over Defendant because it conducts substantial business in Illinois.

7. Venue lies in this District pursuant to 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and Defendant can be found in this District.

RELEVANT FACTS

8. Defendant is a nationwide less than load carrier providing direct logistics services across every region of the United States and internationally.[2]

9. Non-party UKG, Inc. d/b/a Kronos ("Kronos") is a payroll service provider that offers services that include the use of biometric time clocks.

10. When Plaintiff was hired by Defendant, he was required to enroll in Defendant's Kronos biometric system using a scan of his fingerprint or hand geometry so that a digital copy or mathematical template based on his fingerprint or hand geometry could be stored on a database with his associated identity information.

[1]Plaintiff seeks statutory, liquidated damages of $1,000 for each negligent violation of BIPA and $5,000 for each intentional or reckless violation of BIPA and allege that there were not less than 3,000 BIPA violations within the last five years.

[2]https://www.odfl.com/us/en/services.html (last accessed 03/07/2024).

11. Plaintiff Alvaro Amigon ("Amigon") was employed by Defendant at its facility located at 5500 W. 47th Street, Forest View, IL 60638, from July 3, 2012 until August 26, 2022.

12. While working for Defendant, Amigon was required to scan his fingerprint or hand geometry each time he began and ended his working day, as well as each time he clocked in and out for breaks.

13. While working for Defendant, Amigon scanned his fingerprint or hand geometry to clock in and out of Defendant's biometric time clock system no less than four times each working day.

14. Each time Plaintiff used the Kronos biometric time clock, his biometrics were scanned, analyzed, or otherwise converted into digital information that was transmitted to and compared with the database to find a matching copy or template.

15. Once a match was found, the Plaintiff was identified or authenticated, and the time of the scan was recorded.

16. Defendant's Kronos biometric system was used for employee identification, authentication, and to track Plaintiff's time worked.

17. Defendant used, collected, otherwise obtained and/or stored Plaintiff's biometric data for purposes of time tracking and employee authentication.

18. Alternatively, Defendant's biometric timekeeping system used, collected, otherwise obtained and/or stored an encrypted mathematical representation of Plaintiff's specific fingerprint's or hand geometry's characteristics for purposes of time tracking and employee authentication.

19. In either event, Defendant's timekeeping system used, collected, and/or stored unique "biometric identifiers" and/or "biometric information," as both terms are defined below, belonging to Plaintiff.

20. The Defendant failed to inform Plaintiff of the specific limited purposes for which the Defendant collected, stored, or used his biometric identifier or biometric information.

21. Defendant never informed Plaintiff of the specific length of time for which Defendant would use or retain his "biometric identifier" or "biometric information."

22. Plaintiff never signed a written release allowing Defendant to collect, capture, or otherwise obtain his biometric information.

23. On information and belief, the Defendant did not have a data retention and destruction policy at any time during which it was collecting, capturing, or otherwise obtaining her "biometric information."

24. BIPA was enacted in 2008 for the purpose of addressing a "very serious need for protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Session No. 276.

25. BIPA was enacted with the understanding that "the full ramifications of biometric technology are not fully known." 740 ILCS § 14/5(f). The legislature specifically found that persons who have their biometrics taken unlawfully are at increased risk of future injury. *Id.*

26. Biometrics are unlike other unique identifiers used to access finances or other sensitive information. "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the

individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[3]

27. BIPA prohibits private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric information unless the private entity: (1) informs that person in writing that identifiers and information will be collected and/or stored; (2) informs the person in writing of the specific purpose and length for which the identifiers or information is being collected, stored or used; (3) receives a written release from the person for the collection of that data; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying said data. *See* 740 ILCS § 14/15(a) and (b)

28. For BIPA purposes, a "biometric identifier" is a personal feature that is unique to an individual and specifically includes fingerprints. 740 ILCS § 14/10.

29. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based upon an individual's biometric identifier used to identify the individual." *Id*.

30. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS § 14/10.

31. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an identifier that is used to identify an individual. *See id*.

32. Ultimately, BIPA is an informed consent statute. Its narrowly tailored provisions place no absolute bar on collecting, sending, transmitting or communicating of biometric data. For

[3] 740 ILCS § 14/5(c).

example, BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does BIPA limit from whom biometric data may be collected, to whom it may be sent, transmitted, or stored. BIPA merely mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

33. The Illinois legislature concluded that the increased risk of future harm is a compensable loss under BIPA. *Rosenbach v. Six Flags Entm't Corp.,* 2019 IL 123186, ¶ 35, 129 N.E.3d 1197, 1206 citing 740 ILCS § 14/5(c) (noting increased risk of identity theft should biometrics be compromised); *Dillon v. Evanston Hosp.*, 199 Ill. 2d 483, 507, 771 N.E.2d 357, 372 (2002) (finding risk of future injury compensable as an element of damages in medical malpractice case). The legislature's decision is particularly reasonable given that the statute of limitations on BIPA claims presumably runs from the date of the collection of biometrics, whereas the future injury may not occur until after the statute has run.

34. The Illinois Supreme Court has recognized that BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Ent. Corp.,* 432 Ill. Dec. 654, 129 N.E.3d 1197, 1206 (Ill. 2019).

35. Plaintiff was continuously and repeatedly exposed to the risks and harmful conditions created by the Defendant's repeated violations of the BIPA alleged herein.

36. This lawsuit is Plaintiff's one and only chance to obtain compensation for Defendant's violations of BIPA. Depending on how technology evolves years into the future, losing control of and ownership over very personal identifiers could have untold harmful consequences.

37. Plaintiff seeks an award of liquidated damages due to the difficulty in quantifying his harm.

COUNT I

Violation of § 15(a) of BIPA
[Failure to Institute, Maintain, and Adhere to Publicly Available Retention Schedule]

38. Plaintiff restates paragraphs 1 through 37 of the Complaint as if set out here in full.

39. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention - and, importantly, deletion - policy. Specifically, these companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 15(a).

40. Defendant failed to comply with these BIPA mandates.

41. Defendant is a nongovernmental "private entity" under BIPA. *See* 740 ILCS § 14/10.

42. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints or hand geometry) collected by Defendant. *See* 740 ILCS § 14/10.

43. Plaintiff's biometric identifiers were used to identify him and, therefore, they constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

44. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 15(a).

45. Defendant failed to make any written policy establishing a retention schedule and guidelines for permanent deletion of biometric data publicly available.

46. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's biometric data when the purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

47. Defendant did not have a retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA when it collected Plaintiff's "biometric information." *See* 740 ILCS § 15(a).

48. Defendant failed to delete Plaintiff's biometric data when Plaintiff ceased working for Defendant, which is when Defendant's purpose for retaining that data ceased.

49. Plaintiff has never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendant, nor has he ever seen, been able to access, or been informed of whether Defendant would ever permanently delete his biometric data.

50. Defendant knew, or was reckless in not knowing, that the biometric-enabled time clock system it used would be subject to the provisions of BIPA, a law in effect since 2008, yet has completely failed to comply with Section 15(a) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15(a) of BIPA.

51. Alternatively, Defendant negligently failed to comply with Section 15(a) of BIPA by failing to adhere to the reasonable standard of care in the less than load logistics industry with respect to biometric information and the mandates of Section 15(a) of BIPA.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court provide Plaintiff with the following relief:

a. Declaring that Defendant violated Section 15(a) of BIPA;

b. Requiring Defendant to comply with BIPA's requirements for the collection, otherwise obtainment, storage, use, and dissemination of biometric identifiers and biometric information as described herein;

c. Requiring Defendant to destroy biometric identifiers or biometric information pursuant to and in compliance with Section 15(a) of BIPA;

d. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(a) of BIPA pursuant to 740 ILCS § 14/20(1);

e. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(a) of BIPA pursuant to 740 ILCS § 14/20(2);

f. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

g. Enjoining Defendant from further violations of Section 15(a) of BIPA.

COUNT II

Violation of § 15(b) of BIPA
[Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information]

52. Plaintiff restates paragraphs 1 through 37 of the Complaint as if set out here in full.

53. BIPA requires companies to obtain informed written consent from its workers before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS § 14/15(b) (emphasis added).

54. "A party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." *Cothron v. White Castle System, Inc*., 2023 IL 128004 ¶ 24 (internal citation omitted).

55. Informed consent is the "heart of BIPA." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020).

56. Defendant failed to comply with these BIPA mandates.

57. Defendant is a nongovernmental "private entity" under BIPA. *See* 740 ILCS § 14/10.

58. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant. *See* 740 ILCS § 14/10.

59. Plaintiff's biometric identifiers were used to identify him and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

60. Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS § 14/15(b)(3).

61. Defendant did not inform Plaintiff in writing that his biometric identifier or biometric information was being collected or stored, or of the specific length of term for which Plaintiff's biometric identifiers and/or biometric information were being collected, stored or used before collecting, storing or using them as required by 740 ILCS § 14/15(b)(1)-(2).

62. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not obtain a written release authorizing such collection. 740 ILCS § 14/15(b)(3).

63. By collecting, capturing, and otherwise obtaining Plaintiff's biometric identifiers or information as described herein, Defendant violated Plaintiff's privacy in his biometric identifiers and information as set forth in BIPA *each time* the Defendant collected, captured, obtained, stored or used Plaintiff's biometric identifiers or information. *See* 740 ILCS § 14/1, *et seq*.; *Cothron v. White Castle System, Inc*., 2023 IL 128004 ¶ 24. "[T]he plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission." *Id.* at ¶ 30.

64. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with Section 15(b) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15(b) of BIPA.

65. Alternatively, Defendant negligently failed to comply with Section 15(b) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(b) of BIPA.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court provide Plaintiff with the following relief:

a. Declaring that Defendant violated Section 15(b) of BIPA;

b. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(b) of BIPA pursuant to 740 ILCS § 14/20(1);

c. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(b) of BIPA pursuant to 740 ILCS § 14/20(2);

d. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

e. Enjoining Defendant from further violations of Section 15(b) of BIPA.

COUNT III

Violation of § 15(d) of BIPA
[Disclosure of Biometric Identifiers or Information Without Obtaining Consent]

66. Plaintiff restates paragraphs 1 through 37 of the complaint as if set out here in full.

67. BIPA prohibits private entities from disclosing, redisclosing or otherwise disseminating a person's or customer's biometric identifier or biometric information without obtaining consent for that disclosure, redisclosure or dissemination, with limited exceptions, none of which are appliable here. 740 ILCS § 14/15(d).

68. Defendant failed to comply with this BIPA mandate.

69. Defendant is a nongovernmental "private entity" under BIPA. *See* 740 ILCS § 14/10.

70. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant, as explained in detail above. *See* 740 ILCS § 14/10.

71. Plaintiff's biometric identifiers were used to identify him and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

72. Defendant systematically and automatically collected, captured, or otherwise disseminated Plaintiff's biometric identifiers and/or biometric information without obtaining the consent required by 740 ILCS § 14/15(d)(1).

73. By utilizing a biometric timekeeping system (time clock and timekeeping databases), Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated biometric identifiers or biometric information of Plaintiff to at least its payroll company, Kronos, without first obtaining the Plaintiff's consent required by 740 ILCS § 14/15(d)(1).

74. By utilizing a Kronos biometric timekeeping system (time clock and timekeeping databases), Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated biometric identifiers or biometric information of Plaintiff to Kronos without first obtaining the Plaintiff's consent required by 740 ILCS § 14/15(d)(1).

75. By disclosing, redisclosing, or otherwise disseminating Plaintiff's biometric identifiers and biometric information without his consent as described herein, Defendant violated BIPA *each time* there was a disclosure, redisclosure or dissemination of the Plaintiff's biometric identifiers in violation of Plaintiff's rights to privacy in his biometric identifiers or biometric information as set0 forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

76. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute, or otherwise intentionally or recklessly failed to comply with Section 15(b) of BIPA.

77. Alternatively, Defendant negligently failed to comply with Section 15(d) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(d) of BIPA.

78. "[T]he plain language of section 15(d) supports the conclusion that a claim accrues upon each transmission of a person's biometric identifier or information without prior informed consent." *White Castle System, Inc*., 2023 IL 128004 at ¶ 29.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court provide Plaintiff with the following relief:

a. Declaring that Defendant violated Section 15(d) of BIPA;

b. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(d) of BIPA pursuant to 740 ILCS § 14/20(1);

c. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(d) of BIPA pursuant to 740 ILCS § 14/20(2);

d. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

e. Enjoining Defendant from further violations of Section 15(d) of BIPA.

JURY DEMAND

Plaintiff hereby respectfully demands a trial by jury.

Respectfully submitted,

ALVARO AMIGON

/s/ Adam J. Feuer

Adam J. Feuer
Majdi Hijazin
Samuel L. Eirinberg
DJC LAW, PLLC
140 S. Dearborn Street, Suite 1610
Chicago, Illinois 60603
(872) 804-3400
adam@teamjustice.com
majdi@teamjustice.com
sam@teamjustice.com

Nick Wooten
DJC LAW, PLLC
1012 West Anderson Lane
Austin, Texas 78757
(512) 220-1800
nick@teamjustice.com
Lead Trial Attorney

Counsel for Plaintiff